ABSTRACT

An improved encryption and digital signature system and method in accordance with the invention reuses an encryption ephemeral key pair from an encryption process in a digital signature process. The reuse of the encryption ephemeral key pair in the digital signature process advantageously results in reduced byte size of the digital signature and reduction of costly computation overhead. In a preferred embodiment, the invention is based on the El Gamal encryption scheme and the Nyberg-Rueppel signature scheme. The present invention is particularly useful for operation in conjunction with small communication devices having limited processing and storage, wherein such devices may communicate via bandwidth sensitive RF links.